ABSTRACT OF THE DISCLOSURE

A method of reducing power consumption and/or enhancing computation speed in the modulus multiplication operation of a Montgomery modulus multiplication module. A coding scheme reduces the need for an adder or memory element for obtaining multiple modulus values, and the use of carry save addition with carry propagation addition enhances the computational speed of the multiplication module.